UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/682,402	10/09/2003	Kyusun Chang	AUS920030685US1	8362

45371 7590 11/27/2007

IBM CORPORATION (RUS)
c/o Rudolf O Siegesmund Gordon & Rees, LLp
2100 Ross Avenue
Suite 2800
DALLAS, TX 75201

EXAMINER	
LAFORGIA, CHRISTIAN A	
ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
11/27/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/682,402	**Applicant(s)** CHANG ET AL.	
	Examiner Christian La Forgia	**Art Unit** 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 October 2007*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-6 and 8-31* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6 and 8-31* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *09 October 2003* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 29 October 2007 has been entered.

2. Claims 1-6 and 8-31 have been presented for examination.

3. Claims 7 and 32 have been cancelled as per Applicant's request.

Response to Arguments

4. Applicant's arguments, see page 12, filed 29 October 2007, with respect to claim 5 have been fully considered and are persuasive. The objection of claim 5 has been withdrawn.

5. Applicant's arguments with respect to claims 1-6 and 8-31 have been considered but are moot in view of the new grounds of rejection set forth below.

Specification

6. The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter of claims 24-30. The specification fails to provide antecedent basis for "computer usable medium." See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction is required.

Claim Rejections - 35 USC § 101

7. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

8. Claims 24-30 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claims 24-30 are directed to "a program product operable on a computer" embodied on a "computer-usable medium." One of ordinary skill in the art could reasonably construe that the claimed computer-usable medium included both storage media and transmission media such as the Internet. The Office's current position is that claims involving transmission media, such as signals encoded with functional descriptive material, do not fall within any of the categories of patentable subject matter set forth in 35 U.S.C. § 101, and such claims are therefore ineligible for patent protection. *See* 1300 OG 142 (November 22, 2005) (in particular, see Annex IV(c)).

Claim Rejections - 35 USC § 103

9. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

10. Claims 1-6 and 8-31 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Application Publication No. 2003/0041266 A1 to Ke et al., hereinafter Ke, in view of U.S. Patent No. 2002/0165949 A1 to Na et al., hereinafter Na.

11. As per claim 1, Ke teaches an apparatus comprising:

a firewall having a processor and a memory (Figure 2 [block 210], paragraph 0033);

wherein the firewall (Figure 2 [block 210], paragraph 0033, 0034, i.e. firewall does some routing, such as determine the intended VLAN for the packet and attaching an appropriate VLAN tag) is part of a router (Figure 2 [block 205], paragraph 0033) that creates a plurality of

Virtual Local Area Networks (Figure 2 [blocks 230, VLAN1, VLAN2, VLAN3, VLAN4]) using a network switch (Figure 2 [block 225], paragraph 0033);

wherein the network switch is connected to the firewall (Figure 2 [block 225], paragraph 0033);

wherein the memory contains a Virtual Local Area Network rules table (paragraphs 0053, 0055, i.e. policy-based and session-based lookup table, classification policies);

wherein the Virtual Local Area Network rules table allows an administrator to designate a trust level for each of the plurality of Virtual Local Area Networks (paragraphs 0039, 0059-0122, i.e. a user interface that allows a user to set incoming and outgoing policies for the VLANS and authentication policies);

wherein only the firewall is used to protect each of the plurality of Virtual Local Area Networks in accordance with a designated trust level (paragraph 0033, i.e. the firewall **210** acts as a common firewall for all the customers);

wherein the designated trust level is a security level associated with a particular set of rules in the firewall (paragraphs 0018, 0031, 0033, i.e. policies are directed to security policies and security domains).

12. Very little patentable weight has been given to the limitation that discusses wherein a residence time is the time required for the firewall to analyze and either permit or deny a packet, since it is used to define a term used in the next limitation and as such fails to provide any structure that would further limit the claim.

13. Ke does not teach wherein the designated trust level reduces the residence time of the packet in the firewall.

14. Na teaches a plurality of security policies that are prioritized (paragraphs 0023, 0054) and a system for minimizing the packet delay time while it traverses through the various policies (paragraphs 0002, 0018, 0021, 0024, 0046).

15. It would have been obvious to one of ordinary skill in the art to have the designated trust level reduce the residence time of the packet in the firewall, since Na states at paragraphs 0002 and 0018 that reducing the residence time, or delay time as discussed by Na, at the firewall improves the overall performance of the network.

16. Regarding claims 2, 16, 19, 23, 26, and 30, Ke teaches a table defining the relationship between the trust levels, the rules, and the plurality of Virtual Local Area Networks (paragraphs 0053, 0055, i.e. policy-based and session-based lookup table, classification policies).

17. With regards to claims 3 and 11, Ke teaches wherein the firewall comprises a configuration program, wherein the configuration program allows a user to add, delete, or modify the Virtual Local Area Network rules table and a plurality of trust levels in the Virtual Local Area Network rules table (paragraphs 0039, 0059-0122 i.e. a user interface that allows a user to set incoming and outgoing policies for the VLANS and authentication policies).

18. With regards to claims 4 and 12, Ke teaches wherein the firewall further comprises: a security program, wherein the security program analyzes a packet and determines if the Virtual Local Area Network rules table permits or denies the packet (paragraphs 0046-0058).

19. Concerning claims 5, 14, 21, and 28, Ke teaches wherein the security program comprises:

instructions for determining a destination of the packet (paragraphs 0048, 0050, extracting layer 2 and 3 information, including TCP/UDP port information);

instructions for determining an appropriate rule to use to analyze the packet using the Virtual Local Area Network rules table (Figure 5 [block 515], paragraphs 0049-0050);

instructions for analyzing the packet using the appropriate rule (Figure 5 [block 520] , paragraphs 0049-0050);

instructions for determining if the packet is permitted under the appropriate rule (Figure 5 [block 525], paragraph 0051);

responsive to a determination that the appropriate rule permits the packet, instructions for permitting the packet (Figure 5 [blocks 535, 540], paragraph 0051); and

responsive to a determination that the rules deny the packet, instructions for denying the packet (Figure 5 [block 530], paragraph 0051).

20. Concerning claims 6, 15, 18, 22, 25, and 29, Ke teaches responsive to a determination that the rules do not permit or deny the packet, instructions for denying the packet (Figure 5 [block 530], paragraph 0051).

21. As per claim 8, Ke teaches a router (Figure 2 [block 205], paragraph 0033) comprising:

a switch (Figure 2 [block 225], paragraph 0033) connected to a firewall (Figure 2 [block 210], paragraph 0033, 0034, i.e. firewall does some routing, such as determine the intended

VLAN for the packet and attaching an appropriate VLAN tag) and a plurality of computer networks (Figure 2 [blocks 230, VLAN1, VLAN2, VLAN3, VLAN4]); and

wherein the firewall allows an administrator to configure a plurality of trust levels and associate a trust level with each of the plurality of computer networks (paragraphs 0039, 0059-0122, i.e. a user interface that allows a user to set incoming and outgoing policies for the VLANS and authentication policies);

wherein the firewall serves each of the plurality of computer networks in accordance with the trust level associated with each of the plurality of computer networks (paragraphs 0046-0058);

wherein the trust level is a security level associated with a particular set of rules in the firewall (paragraphs 0018, 0031, 0033, i.e. policies are directed to security policies and security domains).

22. Very little patentable weight has been given to the limitation that discusses wherein a residence time is the time required for the firewall to analyze and either permit or deny a packet, since it is used to define a term used in the next limitation and as such fails to provide any structure that would further limit the claim.

23. Ke does not teach wherein the trust level reduces the residence time of the packet in the firewall.

24. Na teaches a plurality of security policies that are prioritized (paragraphs 0023, 0054) and a system for minimizing the packet delay time while it traverses through the various policies (paragraphs 0002, 0018, 0021, 0024, 0046).

25. It would have been obvious to one of ordinary skill in the art to have the trust level reduce the residence time of the packet in the firewall, since Na states at paragraphs 0002 and 0018 that reducing the residence time, or delay time as discussed by Na, at the firewall improves the overall performance of the network.

26. Regarding claim 9, Ke teaches wherein the switch comprises a sub-switch: the sub-switch being assigned one of a plurality of trust levels (Figure 2 [blocks 235], paragraph 0033).

27. Regarding claim 10, Ke teaches wherein the firewall analyzes a packet using some of the rules (paragraphs 0046-0058); and

wherein the rules used in the lower trust levels are excluded from the rules used to analyze the packet (paragraphs 0046-0058).

28. With regards to claim 13, Ke teaches wherein the security program comprises:

instructions for determining the sub-switch location of the packet (paragraphs 0033-0034);

instructions for determining a source of the packet (paragraphs 0047, 0052, i.e. determining if the incoming packet is from a trusted or untrusted interface);

instructions for determining a destination of the packet (paragraphs 0048, 0050, extracting layer 2 and 3 information, including TCP/UDP port information).

29. Ke does not teach determining if the packet is attempting to go to a higher trust level; and responsive to a determination that the packet is not attempting to go to a higher trust level, permitting the packet.

30. It would have been obvious to one of ordinary skill in the art at the time the invention was made to determine whether the packet was attempting to go to a higher trust level, and if it was determined that the packet was not attempting to go to a higher trust level, permitting the packet, since Ke discloses at paragraphs 0039, 0059-0122 a system for configuring the rules and policies of the firewall system. Since Ke discloses a system for establishing rules and policies, the Applicant's determination step would only require routine skill in the art to program into the firewall policy engine.

31. As per claims 17 and 24, Ke teaches a method and program product for analyzing a packet using a firewall which, creates a plurality of trust levels for a plurality of computer networks, the method comprising:

using a single router containing firewall to service each of the plurality of computer networks (Figure 2 [block 210], paragraph 0033, 0034, i.e. firewall does some routing, such as determine the intended VLAN for the packet and attaching an appropriate VLAN tag) by performing the steps of:

determining the destination of the packet (paragraphs 0048, 0050, extracting layer 2 and 3 information, including TCP/UDP port information);

accessing a plurality of rules (Figure 5 [block 515], paragraphs 0049-0050);

determining an appropriate rule to use to analyze the packet (Figure 5 [block 515], paragraphs 0049-0050);

analyzing the packet using the rules (Figure 5 [block 520] , paragraphs 0049-0050);

determining if the packet is permitted under the rules (Figure 5 [block 525], paragraph 0051);

responsive to a determination that the rules permit the packet, permitting the packet (Figure 5 [blocks 535, 540], paragraph 0051); and

responsive to a determination that the rules deny the packet, denying the packet (Figure 5 [block 530], paragraph 0051);

wherein a trust level is a security level associated with a particular set of rules in the firewall (paragraphs 0018, 0031, 0033, i.e. policies are directed to security policies and security domains).

32. Very little patentable weight has been given to the limitation that discusses wherein a residence time is the time required for the firewall to analyze and either permit or deny a packet, since it is used to define a term used in the next limitation and as such fails to provide any structure that would further limit the claim.

33. Ke does not teach wherein the trust level reduces the residence time of the packet in the firewall.

34. Na teaches a plurality of security policies that are prioritized (paragraphs 0023, 0054) and a system for minimizing the packet delay time while it traverses through the various policies (paragraphs 0002, 0018, 0021, 0024, 0046).

35. It would have been obvious to one of ordinary skill in the art to have the trust level reduce the residence time of the packet in the firewall, since Na states at paragraphs 0002 and 0018 that reducing the residence time, or delay time as discussed by Na, at the firewall improves the overall performance of the network.

36. As per claims 20 and 27, Ke teaches a method and program product for analyzing a packet using a firewall which creates a plurality of trust levels for a plurality of computer networks, the method comprising:

using a single router containing the firewall to service each of the plurality of computer networks (Figure 2 [block 210], paragraph 0033, 0034, i.e. firewall does some routing, such as determine the intended VLAN for the packet and attaching an appropriate VLAN tag) by performing the steps of:

determining the sub-switch location of a packet (paragraphs 0033-0034);

determining a source of the packet (paragraphs 0047, 0052, i.e. determining if the incoming packet is from a trusted or untrusted interface);

determining a destination of the packet (paragraphs 0048, 0050, extracting layer 2 and 3 information, including TCP/UDP port information);

wherein a trust level is a security level associated with a particular set of rules in the firewall (paragraphs 0018, 0031, 0033, i.e. policies are directed to security policies and security domains).

37. Ke does not teach determining if the packet is attempting to go to a higher trust level; and responsive to a determination that the packet is not attempting to go to a higher trust level, permitting the packet.

38. It would have been obvious to one of ordinary skill in the art at the time the invention was made to determine whether the packet was attempting to go to a higher trust level, and if it was determined that the packet was not attempting to go to a higher trust level, permitting the packet, since Ke discloses at paragraphs 0039, 0059-0122 a system for configuring the rules and policies of the firewall system. Since Ke discloses a system for establishing rules and policies, the Applicant's determination step would only require routine skill in the art to program into the firewall policy engine.

39. Very little patentable weight has been given to the limitation that discusses wherein a residence time is the time required for the firewall to analyze and either permit or deny a packet, since it is used to define a term used in the next limitation and as such fails to provide any structure that would further limit the claim.

40. Ke does not teach wherein the trust level reduces the residence time of the packet in the firewall.

41. Na teaches a plurality of security policies that are prioritized (paragraphs 0023, 0054) and a system for minimizing the packet delay time while it traverses through the various policies (paragraphs 0002, 0018, 0021, 0024, 0046).

42. It would have been obvious to one of ordinary skill in the art to have the trust level reduce the residence time of the packet in the firewall, since Na states at paragraphs 0002 and

0018 that reducing the residence time, or delay time as discussed by Na, at the firewall improves the overall performance of the network.

43. As per claim 31, Ke teaches a firewall capable of creating a plurality of trust levels for a plurality of computer networks comprising:

a router (Figure 2 [block 205], paragraph 0033) containing the firewall (Figure 2 [block 210], paragraphs 0033, 0034, i.e. firewall does some routing, such as determine the intended VLAN for the packet and attaching an appropriate VLAN tag);

a plurality of rules (Figures 5 [blocks 515, 520], paragraphs 0049-0050, i.e. traffic policies and classification rules);

a table defining the relationship between the trust levels, the rules, and the computer networks (paragraphs 0053, 0055, i.e. policy-based and session-based lookup table, classification policies);

a configuration program, wherein the configuration program allows a user to add, delete, or modify the rules and trust levels in the table (paragraphs 0039, 0059-0122 i.e. a user interface that allows a user to set incoming and outgoing policies for the VLANS and authentication policies);

a security program, wherein the security program analyzes a packet and determines if the rules permit or deny the packet (paragraphs 0046-0058), the security program comprising:

instructions for determining the destination of the packet (paragraphs 0048, 0050, extracting layer 2 and 3 information, including TCP/UDP port information);

instructions for determining the appropriate rules to use to analyze the packet using the table (Figure 5 [block 515] , paragraphs 0049-0050);

instructions for analyzing the packet using the rules (Figure 5 [block 520] , paragraphs 0049-0050);

instructions for determining if the packet is permitted under the rules (Figure 5 [block 525], paragraph 0051);

responsive to a determination that the rules permit the packet, instructions for permitting the packet (Figure 5 [blocks 535, 540], paragraph 0051);

responsive to a determination that the rules deny the packet, instructions for denying the packet (Figure 5 [block 530], paragraph 0051); and

responsive to a determination that the rules do not permit or deny the packet, instructions for denying the packet (Figure 5 [block 530], paragraph 0051),

wherein only the firewall is used to protect each of the plurality of computer networks (paragraph 0033, i.e. the firewall **210** acts as a common firewall for all the customers);

wherein a trust level is a security level associated with a particular set of rules in the firewall (paragraphs 0018, 0031, 0033, i.e. policies are directed to security policies and security domains).

44. Very little patentable weight has been given to the limitation that discusses wherein a residence time is the time required for the firewall to analyze and either permit or deny a packet, since it is used to define a term used in the next limitation and as such fails to provide any structure that would further limit the claim.

45. Ke does not teach wherein the trust level reduces the residence time of the packet in the firewall.

46. Na teaches a plurality of security policies that are prioritized (paragraphs 0023, 0054) and a system for minimizing the packet delay time while it traverses through the various policies (paragraphs 0002, 0018, 0021, 0024, 0046).

47. It would have been obvious to one of ordinary skill in the art to have the trust level reduce the residence time of the packet in the firewall, since Na states at paragraphs 0002 and 0018 that reducing the residence time, or delay time as discussed by Na, at the firewall improves the overall performance of the network.

Conclusion

48. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

49. The following patents are cited to further show the state of the art with respect to residence times as they pertain to firewalls, such as:

United States Patent No. 6,976,089 B2 to Na et al., which is cited to show the patent that issued from the pre-grant publication that was used to reject the claims.

United States Patent No. 7,076,650 B1 to Sonnenberg, which is cited to show selective scanning at a firewall.

50. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (571) 272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

51. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

52. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Christian LaForgia
Patent Examiner
Art Unit 2131

clf